WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Monday, September 12, 2005

Hide?	Set Name	Query	Hit Count
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L24	L23 and "input block"	0
☐	L23	L21 and "nested"	1
☐	L22	L21 and "concatenation"	0
☐	L21	L20 and L12	22
☐	L20	((message authentication code or MAC) near3 (keyed hash function) with (compression function))	61696
☐	L19	L2 and L13	0
☐	L18	L17 same "keyed hash function"	3
☐	L17	"iteration" same "message authentication code"	4
☐	L16	"iteration" same "nested message authentication code"	0
☐	L15	"single iteration" same "nested message authentication code"	0
☐	L14	713/156.ccls.	553
☐	L13	455/411.ccls.	1276
☐	L12	380/258.ccls.	125
☐	L9	380/229.ccls.	43
☐	L8	380/270.ccls.	553
☐	L7	705/67.ccls.	360
	DB=USPT; PLUR=YES; OP=OR		
☐	L6	L5 and "iteration"	0
☐	L5	L4 and "hash"	4
☐	L4	L1 and "message authentication code"	8
☐	L3	L2 and L1	0
☐	L2	"message authentication code" and "compression function" and "hash"	47
☐	L1	380/247.ccls.	169

END OF SEARCH HISTORY

Web Results **1** - **10** of about **237** for **concatenation, compression function, keyed hash function, iteration,**

[PDF] An abridged version of this paper appears in Advances in ...
File Format: PDF/Adobe Acrobat - View as HTML
It allows for a better modeling of **keyed hash functions** as needed ... one **iteration** of the **compression function**. That is, this outer **function** is basically ...
www.cs.ucsd.edu/users/mihir/papers/kmd5.pdf - Similar pages

[PDF] An abridged version of this paper appears in Advances in ...
File Format: PDF/Adobe Acrobat - View as HTML
... **function** F to the **concatenation** of k and x ... **keyed** IV" approachwe can dene **keyed hash functions** as a ... k (x) = f (kx) be the **keyed compression function**, where ...
uncensored.citadel.org/pub/unix/bck2.pdf - Supplemental Result - Similar pages

[PS] An abridged version of this paper appears in Advances in ...
File Format: Adobe PostScript - View as Text
Moreover they use the **hash function** (or its **compression function**) as a black box, ... Theorem 4.1 If the **keyed compression function** f is an (ffl ...
cr.yp.to/bib/1996/bellare-hmac.ps - Similar pages

[PS] This is a Chapter from the Handbook of Applied Cryptography, by A ...
File Format: Adobe PostScript - View as Text
keyed hash functions,whose specification dictates two distinct inputs, a message and a ... One **iteration** of the MDC-4 **compression function** consists of two ...
www.cacr.math.uwaterloo.ca/hac/about/chap9.ps - Similar pages

[DOC] PKCS #12 v1.0: Personal Information Exchange Syntax
File Format: Microsoft Word 97 - View as HTML
The salt and (to a certain extent) the **iteration** count thwarts dictionary ...
Let H be a **hash function** built around a **compression function** f: Z2u ´ Z2v ...
mirror.switch.ch/ftp/doc/ standard/pkcs/pkcs-12/pkcs-12v1.doc - Similar pages

[DOC] PKCS #1 v2.0: RSA Cryptography Standard
File Format: Microsoft Word 97 - View as HTML
Let H be a **hash function** built around a **compression function** f: Z2u ´ Z2v ...
The **iteration** count is recommended to be 1024 or more (see [PKCS#5] for more ...
mirror.switch.ch/ftp/doc/standard/ pkcs/pkcs-12/old/pkcs-12v1draft.doc - Similar pages
[More results from mirror.switch.ch]

Internet Draft Daniel Simon Microsoft Corp. April 1996 The Private ...
Such implementations should allow messages to be **nested** in the obvious way, ...
(A **keyed hash** is simply the application of a cryptographic **hash function** to ...
www.develop.com/books/pws/draft-benaloh-pct-01.txt - 127k - Cached - Similar pages

digital certificate mumbai
keyed hash functions; hopefully ambiguity is limited by context. ... One **iteration** of the MDC-4 **compression function** consists of two sequential ...
services.eliteral.com/ digital-certificate-mumbai/chap9.php - 267k - Cached - Similar pages

[PS] On the Security of Iterated Message Authentication Codes \Lambda ...
File Format: Adobe PostScript - View as Text

I. Introduction **Message authentication code** (MAC) algorithms have received ...
Moreover, because the **compression function** in MD4-based **hash functions** is of ...
www.scs.carleton.ca/~paulv/papers/IEEE.MAC.ps - Similar pages

RFC 2510 (rfc2510) - Internet X.509 Public Key Infrastructure ...
We then group these **functions** in order to accommodate different ... PKIProtection will contain a MAC value **keyed** with this derived symmetric key and the ...
www.faqs.org/rfcs/rfc2510.html - 148k - Cached - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

concatenation, compression functior Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google